

COOP'S TECHNOLOGY DIGEST

-A Timely Report on The World of Communications-

Published as a confidential industry newsletter ten times each year by electronics and technology author Robert B. Cooper. Reports here are source checked for accuracy prior to publication; readers are cautioned to conduct their own verification of data prior to formulating business judgements based upon reports here. Data of unverified authenticity may be so-labelled as a guide to reader caution. The publisher draws upon 42 years of leading edge electronic industry media experience but can be misled by those with clever agendas. Entire content Copyright 2002 by Robert B. Cooper. When lifting material, please be courteous enough to credit source (i.e., "*as reported in Coop's Technology Digest for ...* "). CTD accepts no source payment for publication of information here. Making "extra copies" for staff use without our written permission is a violation of our copyright, whether the entire publication or portions. Reasonable "Replication Rights" are available to those who find the need to "share" contents with non-subscribers. Query to Gay Cooper at 64-9-406-0651. Our objective?

"To keep the bastards honest."

May 06, 2002 - ISSUE 02-05-88

-IN THIS ISSUE-

Murdoch's 30 June "problem" -p. 2; Enron's "friend" Arthur Andersen dismissed by Murdoch -p. 3; News Corp #3 resigns -p. 4; NDS loses round-one in California court -p. 5; NDS gets boot from USA DirecTV security -p. 6; Contagious "accounting" / DirecTV has been lying -p. 7; Popular press reveals extent of Australia's TV piracy problem -p.10; Confused by it all? This will set you straight -p. 11; Hackers coming out of hiding -p. 14; NDS stock plummets after rival encryption plan announced -p. 16; "Uncrackable encryption" - it's all about photons -p. 17; Sky (NZ) door-to-door sales tactics - p. 18; iTV digital's law suit against NDS -p. 18; iTV (terrestrial) digital calls it quits - piracy victim? - p. 19; Canada's "grey market" pay-TV background -p. 19; 7-zip. Canada's grey market pay-TV ruled illegal -p. 20; Royal Canadian Mounted Police go after estimated 700,000 "illegal" dishes -p. 21; Pay-TV sports honeymoon over? - p. 23; Internet by satellite is a bust -p. 23;

Publication note: August 2002, our 91st issue, will be our last for this publication. Renewals at this time are adjusted to reflect issues to that date and not beyond. No new subscriptions are being accepted. Our SatFACTS Monthly plans no such exodus.

REACHING CTD: Telephone (64) (0)9-406-0651; 24 hour fax (64) (0)9-406-1083.
e-mail Skyking@clear.net.nz. Web site: <http://www.apsattv.com> (SatFACTS sub-file)
Next scheduled issue: June 07, 2002

COOP'S TECHNOLOGY DIGEST / SUBSCRIPTION INFORMATION

There are ten (10) issues per year on a schedule dictated by industry events. The readership includes telecommunication industry consultants, state and privately owned broadcasters/telecasters, brown goods importers, retail stockists, installation and maintenance firm personnel, manufacturers, educators, regulatory agency personnel, business investors and Sir Arthur C. Clarke. All copies sent via airmail / Fast Post, world-wide. Annual subscription fee is as follows: Within New Zealand - \$250; within Australia, through AV-COMM Pty Ltd., PO Box 225, Brookvale, NSW 2100 (tel [61]-2-9939-4377 or fax [61]-2-9939-4376). Outside of Australia and New Zealand, US\$250 per year. Outside of Australia, please make out subscription payment and mail to:

Robert B. Cooper, PO Box 330, Mangonui, Far North, New Zealand

Now - Our Ninth Year of Service to the Pacific

COOP'S TECHNOLOGY DIGEST

May 6, 2002 - VOLUME 02-05-88

Signs of the times

In this report:

- ☞ Murdoch says good bye to Arthur Andersen
- ☞ Murdoch decides pricing for sporting events are too high, bails out
- ☞ Murdoch's NDS encryption given boot by DirecTV (USA)
- ☞ NDS loses round one of California court battle with Canal +
- ☞ iTV Digital slams NDS with piracy lawsuit
- ☞ Sky NZ door to door canvassing ("we will keep calling on you until you DO subscribe!")

Are their patterns here? We believe so.

Neil Chenoweth in "Virtual Murdoch" (Random House NZ and Australia; ISBN 0 436 23389 4) wrote:

"Murdoch's (existing) bankers had loaned him large amounts of money with one condition: at 30 June every year, News Corp's total debt could never be more than 110 percent of its assets. The banks imposed this limit because of the natural preference that bankers all around the world have for ensuring that when a loan goes bad, it is somebody else who loses the money. There are two parts to any company: there is the bit the shareholders own, and there is the bit that the banks and creditors own. A balance sheet lists all of a company's assets. If you take away the debt and liabilities from the total assets, what you have left is the part the shareholders own. Essentially, this is what the company is worth. It is called the net assets, or shareholders' equity. Most of this is held by the shareholders in the form of shares, or stock, though some other sorts of securities are sometimes lumped in to be counted as part of the shareholder's equity.

"In the case of News Corporation, the bank's limit meant that on 30 June each year, for every \$100 million of assets on the News Corp group's balance sheet, debt could never be more than \$53 million. The other \$47 million had to be equity of some kind. What the banks did not realise was the large number of things Rupert Murdoch could include in his measure of equity."

"Murdoch has two ways of getting around this bothersome lending restriction. First, his finance director (Richard Sarazen) argued that News Corp's newspapers were worth far more than the modest value assigned to them in the group's balance sheet. And to prove this point, he kept revaluing the newspapers."

Unfortunately for Murdoch, US accounting rules do not allow assets to be revalued upward. However, Australian accounting rules have no such scruples. Over a 3 year period (1984 to 1987) Sarazen wrote up the mastheads of the group's newspapers by (US) \$1.5 billion. And this meant that Murdoch was now allowed to borrow \$1.6 billion - \$1.425 billion more than before the revaluation, based upon Australian accounting procedures.

"Arthur Siskind and the legal team at Squadron Wollenoff (New York) provided the second half of the puzzle. Murdoch now needed to raise (US)\$1.15 billion. Siskind's twist was that instead of treating 'junk bond' money raised by the notorious Michael Milken on behalf of Murdoch as a 'loan', it would be called 'preferred stock' and because it was 'stock', it became an asset."

Siskind, today remaining on the News Corp Board of Directors, would be quoted in 'American Lawyer' describing the fancy financial work as, "an extraordinarily complicated and very unusual financing."

Siskind was also taking advantage of the Australian accounting principle 'rules'. And because Australian rules allowed junk-bonds arranged for Murdoch by Milken to be called 'preferred stock' and because Australia treated such stock as an increase in equity, the (US)\$1.15 billion raised did double duty. It not only brought in \$1.15 billion in new funds, but under Australian accounting rules also allowed News Corp to go out and borrow an additional (US)\$1.2 billion in bank debt.

By the late 1980s, the tangled financial affairs had lost all but the most diligent banking officers. On paper, The News Corporation Limited was an umbrella holding company from Australia. It controlled, directly or indirectly, more than 70 subsidiaries and subsidiaries of subsidiaries. For example, News International was the British operation while News Limited was the Australian operator of newspapers (and ultimately a 25% owner in Foxtel). News America Holdings operated newspapers and magazines in the USA but in all of these operations offshore firms in the Bahamas, Cayman Islands and other tax havens held the majority interest in even News International and News Limited.

Late April 2002 news item:

Arthur Andersen resigned as its auditor. In a press release April 26, NDS said its board approved the move and made Ernst & Young auditor for the year ending June 30. NDS, London, said it hadn't had any disagreements with Andersen. A NDS spokeswoman reached outside the office couldn't immediately say why Andersen resigned or how much NDS paid in auditing fees last year. NDS, which had revenue of \$304 million in 2001, is 80% owned by Sydney-based News Corp. NDS makes software used in conjunction with set-top boxes to protect digital television signals from being stolen by consumers who haven't paid to receive them.

Chenoweth continued:

"The Australian Tax Office had been investigating the News group for at least two years. According to an internal memo dated May 1996, an Australian Tax Office team had examined Australian companies that were 'thought to represent significant FSI (Foreign Sourced Income) risks ... The analysis done resulted in News Limited being classified as high-risk.'

It continued:

"The risk assessment in respect of News Limited shows substantial funds movement from unlicensed CFCs (Controlled Foreign Companies) to listed CFCs."

"Each year hundreds of millions of dollars of News Corporation earnings bounced around some of the most exotic...offshore tax havens. Huge money streams flowed through more than 75 News Corporation companies in the British Virgin Islands, the Cayman Islands, the Netherlands, the Netherland Antilles, Hong Kong and Bermuda. By the time News Corp's profits made it to the balance sheet to be reported to shareholders...most of News Corp's tax bill disappeared. It was 1985 when News Corporation stopped paying tax in any meaningful way."

Australian accounting whiz Richard Sarazen was the architect for the numbers game. He loved numbers and he apparently loved to "sign" his work much as an artist would place his name on a painting. It began with the Australian "profit after tax" entry line in 1987. He did his computations and then filled in the blank: \$A364.364 (million). Having the same sequence of 3 numbers is not impossible of course. In 1988, \$A464.464. 1989: \$A496.496. 1990: \$A282.282.

The odds against 4 years in a row repeating like that were calculated to be one in one trillion (1,000,000,000,000); it was truly extraordinary. In Australia, this was but one line entry of many hundreds. It was the "starting point" for the calculation of tax ("the profit before abnormal items"). The Australian Tax Office looked at each year separately (although others caught the repetitive "numbers") and as for the British and American tax folks, when the Australian dollar amount was recomputed to British pounds Sterling or the American dollar, the exchange rate "wiped out" the mysterious and amazing number sequence. Sarazen was basically saying to tax folks, "up your ass - catch me if you can!"

Sarazen had a disciple, David DeVoe, who from 1991 became the new finance director of News Corp. For that year he reported "profit before abnormals" of \$A391.391, subtracted Minority Interests of \$A70.070 and came up with a profit of \$A321.321 (million). On a roll, he began the 1992 report with earnings before abnormals of \$A530.530. From 1992 onward, News Corp dropped the last three digits in their annual reports (\$A530.530 would then become, simply, \$A530 million).

One would suspect that Sarazen and DeVoe played this game out of a matter of some pride. They knew they were working with bogus numbers, why not make them unique and a "signature" of their presence? Of course there were three groups who had a keen interest in what the News Corp numbers "really" were. From 1992 to 1997, News Corp had a total reported profits of \$A5.8 billion. That's in Australian dollars and under Australian accounting rules. This was the number reported to the press and to stockholders in the many News Corp divisions. *It had an impressive ring to it.*

When the same accounting team handed the records over to the US accounting team, a new report had to be prepared for the rather stricter rules of the Securities and Exchange Commission. Under US rules, approximately half of the earnings disappeared, even when left in Australian dollars; \$A3 billion remained because in the US News Corp was able to factor in new television broadcast and satellite start-up costs which did not affect the Australian numbers. In Australia, News Corp treated the losses as an asset and capitalised them (not unlike the Arthur Siskind plan for the junk bonds) whereas in the United States these expenditures were written off as a cost.

That deals with the Australian, US authorities and the stockholders but what about the tax man? In that same six year period (1992 to 1997), News Corp companies paid \$A351 million in tax. A big chunk of change? Yes, but.

But - the tax rate averaged 35% for corporate earnings through that period and \$A351 million was 6 percent. Somehow News Corp had managed to avoid paying taxes on \$A4.8 billion. Which brings us back to the 75 News Corp controlled firms in tax havens spread around the globe.

Chenoweth: "It was the next best thing to magic. By a strange alchemy, each year hundreds of millions of News Corporation earnings bounced around the world, touring the archipelagos of offshore tax havens."

Was it illegal? Possibly not. Was it outrageous? Probably yes. Was it suspicious? Well, if you begin with the amazing sequence of numbers created by Sarazen and later Devoe, and those are the "foundation numbers" from which all other calculations develop ... yes, it was (and remains today) suspicious.

Only Israel seems to have called News Corp's number on this one. On April 3, 1998, after a well publicised tax office raid on the NDS (smart card) subsidiary in that country, News Corp announced a US\$3 million "settlement" with the Israel Income Tax commission.

News item (January 23, 2002):

"The number three executive at News Corp, Chase Carey, resigned from the company effective today. In a prepared statement, Rupert Murdoch expressed 'great regret' over Carey's resignation, which was described as voluntary. Carey was COO (Chief Operating Officer) of News Corp and had run the Fox Television Network (USA)."

Arthur Andersen, the accounting firm, has been the primary outside auditor for News Corp for decades. A suspicious person might weigh the plurality of offshore bank accounts, the 75 subsidiary firms mostly unlisted, and the unusual methods employed to retain News Corp subsidiary stock market values and draw conclusions based upon the late 2001 failure of American energy company Enron; *also* a client of Arthur Andersen. What the public has been told about Enron's use of offshore controlled corporations as havens to hide debt, and what researcher Chenoweth has revealed about News Corp raises eyebrows. There are distinct parallels here.

One of the most difficult to unravel is the method used by News Corp (and others of a similar size) to "control" the stock price of shares held by the public. By using offshore controlled corporations, when a stock share value begins to dip, it is possible for a corporation to buy back its own stock on the open market at pricing which is designed to keep the stock value artificially high. This becomes more important when the stock value is deemed critical by the banks (as lenders) in an annual analysis such as The News Corporation faces each June 30th.

As June 30th approaches each year, the accounting firm charged with the final accounting process must somehow make the numbers conform to the demands of the lenders. A ten cent (per share) rise in a stock when 60% of that stock is held by a subsidiary of News Corp here, a \$1.00 rise there can make the difference between meeting the bank's lending criteria and failure to do so. The public perception of the stock's value becomes critical to the lending requirements.

Chenoweth: "As Citibank (as lead lender) had found, the archipelago of tax havens allowed Murdoch to channel The News group's money streams away from the high-tax areas like the US, Britain and Australia. It also made News Corp's corporate structure unbelievably complicated. And that complexity discouraged Murdoch's bankers from wanting to liquidate assets because the ownership was so hard to unravel."

Arthur Andersen's credibility because of the Enron scandal has dropped to all-time low levels. For Murdoch's banks, having Arthur Andersen "sign off" on the June 30 (2002) financial statement could be worrisome and a red flag to the marketplace.

Chenoweth: "No matter how great a media organisation's reach or power, no matter how many countries or deals in which it is involved, (News Corp) remains intensely vulnerable in one area; public confidence. There is not merely a matter of maintaining the confidence of its bankers - though even here News is struggling. It is also a question of probity. Broadcasting licences around the world are granted on the basis that regulatory authorities believe a media group is fit and proper to be entrusted with such a licence. It is a position of public trust. Any accusation that it is involved in illegal activities, even if the accusation is baseless, poses a threat to the group's future."

Follow-up: NDS accused of "hacking" Canal + smart card technology

It sounds like a script once rejected by Hollywood. The plot revolves around two of the world's biggest multinational corporations, locked in an all-out war over the future of pay-TV, and its promised billions. The competition is so ruthless that eventually, someone cheats. One company hires hackers to break the other's secret codes, then publishes the secret on the Internet, inviting piracy. Suddenly, the victim company's pay-TV is free, and its only asset is worthless. Too ruthless to be true? Not according to a lawsuit filed in California in March.

Consider it a new form of corporate espionage. Stealing your competitor's secrets to cash in on them is as old as commerce itself. But stealing your enemy's secrets and giving them away, thereby diluting or eliminating their value? That seems to be a new corporate weapon born of the Internet age. Publishing the Colonel Sanders' secret recipe online would be one thing; but publishing the keys to a pay-TV kingdom is quite another. Hacking pay-TV systems has been sport for hundreds of thousands of video pirates around the world for more than a decade. All that stands between a TV viewer and free programming is a "smart card" inserted in a DirecTV-style set-top box. Crack the secret code in the card, make your own version, and TV is free. In fact, during a day notoriously known as "Black Sunday" in the piracy community, DirecTV effectively zapped some 200,000 piracy cards around North America by sending destructive computer code at them. However widespread, TV piracy has always been viewed as the work of hobbyists. Until last month. In a lawsuit filed March 11 in California by French-based Canal Plus Technologies, a division of Vivendi Universal, the company claims just such chicanery by a division of Rupert Murdoch's News Corp, named NDS. Canal Plus says NDS hired a team of hackers who broke its smart card codes, then distributed the secret on a well-known piracy Web site. The impact on Canal Plus was staggering — sources inside the firm suggest somewhere between half and three-fourths of all Canal Plus users in Italy were pirates, for example. The lawsuit is proceeding apace and a California judge granted Vivendi's request for an accelerated discovery schedule.

NDS said in a statement last month that the charges are baseless, and in fact were used recently as leverage for merger talks. The company declined to say more to journalists. But sources in the computer underground say NDS has at times been "too friendly" with pirates. In fact, there are accusations that NDS employs many computer hackers, including the hacker who developed the first widely-used counterfeit smart card in the early 1990s. NDS has reportedly admitted to partially funding another underground Web site, Thoic.com, but said it did so only for intelligence-gathering purposes. In a deposition during April consultant Oliver Kommerling — who has worked for both Canal Plus and NDS — directly accused NDS employee Chris Tarnovsky of ensuring the smart card code was published on piracy Web site dr7.com in March of 1999. Kommerling's "whistleblower" testimony carries significant credibility because NDS owns 60 percent of his security firm, ADSR. In his statement to the court, Kommerling said he feared repercussions for speaking out. He wouldn't offer additional comments, other than to say in an e-mail, "As I said in my statement about the pressure.....In fact, this has already started."

But the stakes may be even higher. In a declaration filed with the court by Canal Plus security manager Gilles Kaehlin, Kaehlin says Tarnovsky admitted NDS was behind the smart card hack, and that he was prepared to tell the truth in court. But, the filing says, Tarnovsky refused to be the whistle-blower on NDS' illegal activities, "because he feared too much for his life and that of his family," Kaehlin said. None of Canal Plus' allegations have been proven, and NDS has offered a plausible alternative explanation — that their rival's smart cards were simply easy to hack, and that's why the pirates had a field day. But the case is the first high-profile, public look inside a world many computer security experts once only talked about in hushed voices. While graffiti-style Web-page

hacks and other nuisance attackers get most of the press attention, high-stakes hacking — information-age corporate espionage — has been going on silently for some time. It's carried out by criminals too smart to get caught, with too much money and stock value at stake for corporations to come clean when victimised.

There is only a trickle of information available on digital corporate espionage. The most authoritative seems to be an annual survey conducted jointly by the Computer Security Institute and the FBI. Released April 7, the anonymous survey of 500 companies and government agencies revealed once again that cyber espionage is soaring — theft of proprietary information cost the group some \$170 million. But little is known about what kind of information was actually lost. "People have struck up online friendships with employees and then lured them into conspiracy to commit espionage. People have put bounties on laptops of executives. People have disguised themselves as janitors to gain physical access," said Richard Power, editorial director for the institute. But would they steal a rival's proprietary product and give it away, just to make it worthless? "Do not underestimate stupidity and greed. Look at Enron," Power said. "If company executives could participate in that kind of activity and cover it up it is quite plausible they would engage in the kind of activity charged in this case." In fact, Power said, the only thing unusual about this case is the fact that the victim has gone public.

The idea of diluting a rival's value isn't completely without precedent, said Tom Talleur, another cyber-espionage expert with KPMG Consulting Inc. Five years ago, rival Internet service providers would bombard each other with traffic in a denial-of-service attack to make surfing sluggish, and thus entice customers to switch. Two years ago, an Internet hosting provider was accused of hacking into a competitor's customer database, publishing the data online, and then e-mailing the customers with the claim their competitor wasn't secure. The claim was never proven. "Internet technology is so ubiquitous, all you've got to do is sit down and think about 'How can I destroy my competitor?' and you can do it," Talleur said. "This is not a far-fetched notion. I've seen competitors do this to each other. It's not far-fetched at all." Ira Winkler, chief security strategist at Hewlett-Packard Co., said it is standard corporate practice to disassemble competitors' products immediately after they arrive on the market — and what happens to that information is a legal question that's yet to be settled. "Once a car is sold to the public every car manufacturer in the world knows the first buyers are competitors, who tear the car apart bolt by bolt and see how it works," Winkler said. "There are more than enough indications this has gone on. Reverse-engineering your competitors' practices is standard practice. 'If industries start doing this as general practice, put on their corporate Web site 'Here's how to steal services from my competitor,' well, is there anything illegal about detailing how you can rob a bank? No, but do you want to be known for that?'"

The court of public opinion may very well be the ultimate arbiter. Canal Plus and Vivendi have even bigger problems right now than hackers. Vivendi Chairman Jean-Marie Messier was already under fire because the firms' slumping stock price, but things got nasty when he fired popular Canal Plus chief executive Pierre Lescure. Lescure founded Canal Plus and his ouster was viewed as disloyal; it's prompted broadcast interruptions by protesting Canal Plus employees. And it's even become an issue in the French presidential campaign.

All the chaos adds fuel to claims that Canal Plus lawsuit is really just sour grapes, a desperate move by a company that's simply being beaten in the marketplace. But if Canal Plus lawyers follow through on their promise to march a series of underground computer hackers to the witness stand in California, all to make ugly claims about who really funded their work, News Corp might suffer an even more serious blow to its reputation. Any company found guilty of performing this kind of piracy would be putting its reputation on the line," said Bill Malik, an analyst with KPMG. "Corporate integrity is primary, especially when you're not talking about some physical goods, you're talking about something like content."

Hard on the heels of the Canal + suit, NDS received some more bad news. The world's largest satellite pay-TV service, DirecTV (USA) owned by General Motors, after 7 years of depending upon NDS for "security" and "protection" was kicking the Murdoch subsidiary out. This report.

NYC Loves its FREE DirecTV. HEY buddy, want free satellite television? That question plagues DirecTV, the nation's largest provider of satellite television programming. The company faces an uphill battle as it fights a market for illegally modified access cards. The hacked cards allow end users

to watch everything from movies and concerts to NFL and NBA games - without paying a dime. And if what The Post has seen in New York is any indication, the company has its hands full. Of the 25 bars and restaurants The Post visited in two Brooklyn neighbourhoods, representatives of 11 establishments admitted to stealing DirecTV programming. Additionally, The Post had no problem finding people who sell and use hacked access cards. Among those who admitted to stealing DirecTV programming were local law enforcement officers, lawyers and business executives.

"It is a very serious problem, and we devote serious resources to it," Larry Rissler, vice president of signal integrity for DirecTV, told The Post. "We can't quantify how much money we lose, but at some point it will probably cost the consumer more because the cost associated [with combating piracy] is significant." Rissler, a former FBI agent, is DirecTV's top cop and is in charge of fighting piracy.

DirecTV's problems were recently highlighted when WFAN personality Sid Rosenberg appeared on the "Imus in the Morning" program and admitted that he uses a modified access card. DirecTV was listening, and it slapped Rosenberg with a lawsuit for violating the Digital Millennium Copyright Act. While Rosenberg's apparent admission of guilt was brazen, he's not alone. A network of traffickers across the New York area allow anyone, for around \$300, to get their hands on a hacked DirecTV access card. The cards usually carry a guarantee so that if DirecTV disables the card, the seller will reprogram the card for the buyer.

DirecTV bombards its receivers and cards with electronic countermeasures (ECMs) to disable them. But users buy cards and equipment online from businesses operating in Canada. Rissler says DirecTV is gearing up to release a fourth version of its access cards with new encryption codes it hopes will make it harder to modify the cards. The company also hopes a Canadian law currently under review will make it illegal for companies to sell cards and equipment to reprogram the cards.

But one person who uses hacked access cards at home and at his business says it may not matter much. "I think 25 percent of people with DirecTV have never paid the company a dime. No matter what the company does, someone will figure out how to break the codes, and new cards will be out on the street."

DirecTV Swaps Smart Cards. DirecTV Inc. admitted that it has begun distributing replacement smart cards that provide conditional access to programming for its more than 10 million direct-broadcast satellite customers. The swap-out marks the fourth-generation of smart cards since the service launched in 1994. The company also confirmed that it will transition its conditional-access technology away from its initial provider, NDS Group plc, and take it in-house.

DirecTV's engineers were largely responsible for the new smart-card design, spokesman Bob Marsocci said. NDS admitted in a statement that DirecTV began the transition to its own technology. It added that the companies' contract remains in force until August 2003, and NDS will continue to generate revenues from its DirecTV relationship until then.

DirecTV plans to mail more than 15 million smart cards over the next six months. It has set up a dedicated on-air channel to instruct customers how to replace the cards in their DBS receivers. Periodic smart-card swap-outs have become mandatory thanks to aggressive DBS-signal pirates who alter smart cards that allow them to access programming, including seasonal sports networks and pay-per-view movies, free-of-charge. Electronic countermeasures sent via satellite have helped to curb, but not eliminate, the piracy.

DirecTV, a subsidiary of Hughes which is owned by General Motors, has its own "honesty" problem going. In mid-April, the pay-TV provider sent shock waves through the financial world by admitting it had "prematurely counted" new subscribers. The following report clarifies.

Hughes Electronics and its DirecTV unit reported results for the first quarter, numbers that included a record number of DirecTV gross subscriber additions for the three-month period but a change in the overall subscriber count for the satellite TV service. During the three-month period, DirecTV added 849,000 gross subscribers. Executives said that 849,000 reflects the best ever figure in terms of gross additions for any first quarter. After accounting for churn, the service enrolled 342,000 net customers for the quarter. However, Hughes and DirecTV reduced the satellite TV service's cumulative subscriber base by approximately 360,000 to take into account customers previously identified as pending subscribers. That took the satellite TV service's total to 10.56 million. Beginning with the first quarter, DirecTV said it no longer will include pending subscribers in its cumulative subscriber base. Pending subscribers are customers who have purchased equipment and have had all of the

required customer information entered into DirecTV's billing system, but have not yet activated service. Executives said the new policy reflects a more simplified and conservative approach to counting customers, and is consistent with the rest of the multichannel television industry. DirecTV President Roxanne Austin added that the switch is part of a larger overhaul of operations at the satellite TV unit. Austin said the change has no impact on DirecTV's past or future revenues, EBITDA or cash flow. As for the rest of 2002, Austin said DirecTV expects to add 1.2 million customers this year for its core business, an estimate that's independent of the National Rural Telecommunications Cooperative's DirecTV business. Austin also said 70 percent of new subscriber additions in the 41 cities that get local TV channels from DirecTV are taking the company's local TV packages. Hughes said first quarter 2002 revenues increased 7.7 percent to \$2.038 billion, compared with \$1.893 billion reported during the same period in 2001. EBITDA for the quarter was \$134.2 million, compared with first quarter 2001 EBITDA of \$113.2 million. The first quarter net loss was \$156.4 million, compared to a net loss of \$105.3 million in the same period in 2001.

Hughes Picks Up Strong Static For Inflating Subscriber Data. Satellite broadcaster Hughes Electronics Corp., which built its reputation and share price on soaring growth, suddenly is running into turbulence for having inflated subscriber numbers over the years. Hughes raised eyebrows among many investors and analysts this week by announcing an abrupt change in the way it counts and reports closely watched quarterly and year-end subscriber totals. The company disclosed that, since 1995, its flagship DirecTV unit routinely included as part of its subscriber base certain customers before they ever started receiving the service or paying for it. Among other things, for many of those years, Hughes counted people who filled out applications but may have put down only a small deposit and perhaps left no credit card. At least some of these potential customers walked away before they ever paid a dime, though it isn't clear exactly how many; Hughes maintains at least four out of five ended up producing revenue.

The practice pumped up a key figure watched by Wall Street to value Hughes shares, a tracking stock of parent General Motors. But in one fell swoop, Monday's decision to stop taking credit for this backlog of "pending" subscribers cut about 360,000 homes from what DirecTV previously said was a more than 10.7 million total ratepayer base. The move toward a more-conservative methodology comes amid a controversy swirling on Wall Street about accounting practices in the cable-television sector, most notably at Adelphia Communications. There, the company recently disclosed that it had \$2.3 billion in off-balance-sheet, co-guaranteed debt. Given Wall Street's post-Enron Corp. jitters and hypersensitivity regarding any type of accounting hiccup or reporting discrepancy, Hughes management now finds itself on the defensive, answering questions about whether it has been unduly aggressive in claiming subscriber additions. The El Segundo, Calif., company acknowledges that no other satellite-broadcaster or cable-TV provider used its now-jettisoned methodology.

Hughes officials stress that the subscriber shift wasn't prompted by any outside pressure and won't affect previous earnings. Hughes, whose main asset is DirecTV, has consistently racked up losses as a result of the high cost of snaring new subscribers and building up a critical mass in the marketplace. Spokesman George Jamison says the decision by Hughes to disclose for the first time the full details of how it accounts for new subscribers "adds simplicity and clarity" to Hughes's results. "There's nothing in any of this that's improper" or will negatively affect cash flows or other financial details reported in the past, he adds. Suddenly halting the practice produces a big one-time hit "only if you freeze or merge the business." Executives maintain that the change merely eliminates practices that have "outlived their usefulness" as the company has grown 20-fold since the mid-1990s, and the backlog of subscribers waiting to be activated has swelled accordingly. Hughes's "operating statistics may not have been perfect," concedes Mike Palkovic, DirecTV's chief financial officer, but he adds: "I don't believe we misled any investors." Indeed, on Monday the company also reported better-than-expected financial results, subscriber additions and revenue figures per household, and it ramped up by 20% projected net subscriber additions for the full year. Echoing the sentiments of other fund managers, Mitch Julis of Canyon Capitol Advisors, a Beverly Hills, Calif., hedge fund, gives management a backhand compliment for cleaning up the books in anticipation of the merger with EchoStar Communications. Despite the subscriber dip, Mr. Julis maintains that Hughes stock is still "a very compelling offer" for investors, compared with shares of cable-TV companies, because of its comparatively low debt and the "attractive upside potential" of the pending merger. Nonetheless,

neither the market, nor many analysts, were thrilled with the disclosure. The company's shares slumped nearly 3%, though they regained ground in a strong market rally. Further clouding Hughes's market performance: the widespread perception that its pending combination with smaller rival EchoStar may be blocked by federal regulators. Still, the shares have outpaced the broader market since the announcement of the EchoStar pact in late October. The adjustment by Hughes "wasn't a mind-blowing number, but it was significant enough that they needed to step forward and make the correction," according to Ford Cavallari, global practice leader for Adventis, a telecommunications consulting firm in Boston. "I certainly wouldn't give them an A grade" for past reporting criteria, he says, adding that with investors' suspicions high and quarterly reports generally under microscopic examination every quarter, smart companies now realise "they would be well advised to do a mea culpa before" outsiders demand changes.

According to Hughes, the practice of rolling "pending" subscribers into its customer base was initiated to better reflect the underlying growth rate of the fledgling company, particularly factoring in the lag between customer sign-up and activation of DirecTV's service. That pending number started at a moderate 40,000 level in 1995, but as internal criteria remained unchanged, it climbed to a peak of 345,000 by the end of March 2000, when the company enjoyed skyrocketing growth. Those up front financial commitments are now significantly greater for customers, and the "pending" category has remained essentially flat for the past five quarters. But in response to questions, Hughes acknowledged that between March 1999 and March 2000, for instance, DirecTV's overall rolls effectively were inflated by about 200,000 customers, or about 10% of the total net subscribers the company took credit for in that period. For some investors, the size of the subscriber adjustment Hughes disclosed this week emphasised management's past mistakes and continuing shortcomings. "It highlights the advantages EchoStar's management team can bring to the table in a combined company," says Douglas Eby, president of Toray & Co., a Hughes holder. Through his spokesman, Hughes's chief executive officer, Jack Shaw, says he personally "insisted" on the change to get "in line with what he promised investors he would do" to reinstall discipline and reliability in the company's operations. Since no revenue was imputed to the removed subscribers, Hughes won't have to restate its most important measures of financial health, including the metric favoured by Wall Street: earnings before interest, taxes and certain other ordinary business items. Furthermore, taking out those extra customers actually improves the average return per subscriber, another item closely monitored by Wall Street. Still, in future filings with the Securities and Exchange Commission, Hughes will have to take the embarrassing step of restating its subscriber numbers, going back to the beginning of last year.

Coop's comment: In New Zealand, the programme supplier (Sky) is the only source for set-top (IRD) units. In Australia, Foxtel or Austar's installation people deliver the set-tops as a part of the installation process. However, in the UK and USA, set-top boxes are "sold" to would-be subscribers through a variety of electronic and merchandising outlets. For the price of a set-top package, the consumer can walk out of the selling shop with a complete system under their arm. And if they are so inclined, install it themselves.

DirecTV, Echostar/Dish (USA) and BSkyB have taken this sell-through approach to reduce their own subsidised investment in set-top boxes. Sky, Foxtel and Austar have taken a different approach and carry the full cost of each set-top on their books.

The advantage to being the sole source for set-tops should be obvious; the only boxes in the hands of consumers are those boxes that go through your own inventory control system. And step-one for any would be "grey market" (piracy card) user is to get his or her hands on a set-top box.

What appears to have been missed in the sudden burst of "honest accounting" at DirecTV is the obvious relationship between piracy sourced smart cards and the "mysterious" 200,000/340,000/who-really-knows how many" missing set-tops. DirecTV relates there were various reasons why people who acquired boxes did not end up as paying subscribers. In their press statements, they try to suggest that people who "did not leave a credit card may have been miscounted" as potential buyers. In fact, this is how it works (Mr. Creagh is a Canadian, and you will see why we have selected his "story" shortly.).

Pat Creagh thought space was the final frontier. So he went stateside last fall to pick up a \$50 US satellite dish at Wal-Mart. He had it wired, pointed it at Texas and entered a 700-channel TV universe. "I had about \$300 invested with the hook-up and everything, and

with the amount of movies, I was getting my money back quite nicely," said the man behind Creagh & Coe Hairstyling on James Street South (Hamilton, Ontario, Canada). Creagh saved money by scaling back his cable TV plan, while his dish and converter brought him all the sports and uncut movies he could want. He visited Arc Satellite whenever his signal was "zapped" and his "HU" access card needed descrambling. But when his U.S. signal started going screwy more and more often, he knew the end was near. The end arrived yesterday when up to a million Canadians like Creagh were branded thieves after the Supreme Court ruled it is illegal to decode satellite TV signals beamed into this country from abroad.

So you walk into a shop selling set-tops, buy the boxed system and take it home. The selling store has taken your details and has a record of who you said you are and where you said you live. If you paid by credit card, they also have a way to "trace" (verify) your basic identification and address details. Once home, you have three choices: (1) Contact DirecTV (or DISH) and with your system installed request service. At that point you are a paying subscriber. (2) Install the dish but obtain a grey market smart card. The system now functions, but at DirecTV you are a "pending subscriber" who in fact will probably never become a "paying subscriber". This is the 200,000/340,000/??? knows number DirecTV has eliminated from their books. (3) Stick the set-top in a closet and forget about it.

All set-tops have unique serial numbers, recorded at the time of sale. All smart cards have unique serial numbers, recorded at the time the card is supplied to the subscriber. The two number sets are held as "one file" when a set-top box activates as a paying subscriber.

DirecTV's "honesty" could have been more honest. It could have admitted that because set-tops are marketed "openly" this creates a scenario for piracy. Alas, they did not do this. Meanwhile in Australia, while Foxtel and Austar attempt to control set-top box sales, in fact their Irdeto (version 1) encryption system invites grey marketing sourcing of Irdeto capable receivers from alternate sources; often in Europe. If the USA and Canada have upwards of 25% of all satellite pay viewers using piracy cards, the percentage in Australia would be lower - perhaps 7% - a direct result of the lack of home dish system packages at retail stores; that first step which with a poorly designed security system (such as the NDS VideoGuard in the USA or Irdeto 1 in Australia) ends up being a piracy headache. This report.

Show Stealers. Pay-TV piracy is also on the rise in Australia. But, as Joshua Gliddon discovers, there's precious little the providers can do - having a dodgy connection is not technically illegal.

A conversation overheard at a bus stop: "It's dead easy. I just asked around and found someone to sort it out. It cost me about a grand." Another conversation, the same day, a world away in an elevator: "Mate," says the suit, "there's nothing we can do about it. There are so many cards and boxes floating around out there." His fellow traveller just looked at him.

They're all talking about pay-TV piracy. It's been going on in the United States for years, but in Australia, it has been very hush hush. Until now. Cable-TV piracy is on the rise, boosted by easily available satellite dishes from the Galaxy collapse, legitimate set-top boxes and an entire army of electricians, installers and pub salesmen willing to hook you up for minimal dollars. Australian households access pay-TV using either the hybrid fibre cables strung through metropolitan areas, or via satellite feeds. On top of that are thousands of "dead" connections - satellite or cable hook-ups no longer in use because the householder has moved on or allowed their contract to expire.

The pay-TV industry in Australia has been labouring under the huge costs caused by rolling out their cable networks and by the unfavourable contracts they negotiated with American studios. Lower-than-expected subscriber numbers haven't helped either. Only 20% of Australian homes have pay TV, and it accounts for only 10% of all TV hours watched in the nation. The proposed agreement between Foxtel and Optus will help alleviate the industry's burden, but dodgy, non-revenue-paying connections certainly don't help.

"It's not actually illegal to have an unauthorised pay-TV connection," says Debbie Richards, a spokeswoman for the Australian Subscription Television and Radio Association (ASTRA). "We lobbied hard to have the Copyright Digital Agenda Bill include cable piracy as an offence, but it did not happen." Richards says she suspects that the government wasn't keen to implement a law that would enable pay-TV providers to "kick in the doors" of people suspected of having an illegal hook-up. "If you facilitate the connection, then you're committing an offence. But receiving the illegal connection is fine under the current law."

So who's doing the dodgy connections? Roger (not his real name) is an electrician. He's done 20 or so illegal connections in the northern Sydney metropolitan area, and has a stash of satellite dishes and decoder boxes in a backyard shed. He's understandably cagey about being identified. "I don't promote it," he says. "I don't go down to the pub and tell people that I'm the man for the job. But it's like anything: if people want something badly enough, then they'll ask around. And if they ask, they'll probably get referred to me." Roger charges about \$1000 to do the hook-up and isn't the only cagey person in this story. Foxtel and Optus representatives are understandably concerned about giving cable piracy too much publicity. "We're not in the business of giving cable piracy tutorials," says Foxtel's director of corporate affairs, Mark Furness. "Suffice to say we've got people out there investigating [the piracy], and there have been prosecutions."

While it's impossible to estimate the number of dodgy connections, what's certain is that most are satellite, rather than cable. There's a simple reason for this: it's easier to point a dish at the sky than it is to splice a cable into a set-top box. Optus doesn't have a satellite service and anecdotally reports a lower incidence of piracy. Company representatives told The Bulletin that because the HFC cable system works in similar ways to ethernet computer networks, getting a dodgy connection requires technical nous and the ability to physically fiddle with the electronics in the set-top box. It also means that the house must have been cabled at some point in the past. Satellite is easier because there's no cable.

The signals beamed down from the satellite are scrambled; when they hit the dish, they're routed down a cable and into a set-top box which uses a smart card to descramble the signal and create a viewable picture. In an effort to beat the pirates, pay-TV providers typically change the way their signals are scrambled, which confuses the smart cards in illegal connections and renders them unable to descramble the signal. Richards says there are stories about people calling up the customer service centres [of pay-TV companies] and asking why they're not getting a picture when their connections have been illegally facilitated.

Are people really that silly? Furness takes up the story. "What seems to happen is that hubby heads down to the pub, picks up a hot box and smart card and takes it home, telling the wife that they've now got cable. Then we scramble the signal and the picture is no longer coming through. The wife calls up customer service and is pretty surprised to find out that it's not a legal connection." Sounds like something out of Andy Capp, but the various pay-TV players swear it's true.

Furness emphasises that people are stitching themselves up by handing over cash to the black marketers. But what he probably doesn't know, or isn't telling, is that there's a thriving underground market in re-keying the smart cards used in set-top boxes. The friendly electrician Roger notes that there are a couple of people he's aware of who do overnight turnarounds on hot smart cards. "So the signal gets scrambled, and what happens is that there are guys out there you send your smart card to. You pop it in an express-post envelope and send it off. If you put another envelope in there, and include 20 bucks, you'll have the new card back in a day or so."

There is also anecdotal evidence that suggests there are set-top boxes that can't be fooled by scrambled signals, but if that's the case, the pay-TV companies aren't talking. Roger also suggests that the scrambling is changed more frequently in metropolitan areas than in the country, but given that it's all one signal coming down from the satellite, there's a good chance he is wrong.

So there are some who find it all very amusing, doing the pay-TV companies out of cash. After all, it's almost unAustralian to disapprove of sticking it up the big guys. And the fact that it's not illegal to receive a dodgy signal makes it even more tempting. The problem is that morally, if not legally, it's wrong. What's more, if ASTRA has its way, it will be illegal to receive black market cable. The real question is, who's the loser?

Excellent summary

Of all of the analysis of how NDS versus Canal + plus DirecTV + Canadian grey market dissolves into a single world-wide challenge, this report is the best we have found. It was built by accessing the Canal Plus web site (www.actionone.com) which has posted on a daily basis the new depositions the French firm has obtained in preparing for the initial California court hearing.

Breaking the pay-TV code-breakers. The real drama unfolded unnoticed on this happiest of days, half a world away. It was March 27, 1999, and in Australia all eyes in the media were focused on the Murdoch family property Cavan, near Canberra, where as rain fell steadily, Lachlan Murdoch married

Sarah O'Hare. With Rupert and Anna Murdoch in the last throes of an acrimonious divorce, most attention was on the awkward family groupings. What no-one at Cavan knew was that, on the other side of the world in British Columbia, where it was still March 26, a Canadian hacker called Allen Menard was posting a computer file on his website, DR7.com.

Three years later that file, titled Secarom.zip, is a \$US3 billion (\$5.6 million) headache for the Murdochs. The multibillion-dollar question is, where did Menard get the file? French media group Canal Plus says the answer lies somewhere in the records of NDS Group, a technology outfit that must have one of the most colourful and bizarre histories of any listed company. On March 12 this year, three weeks after Lachlan joined his brother James on the board of NDS (in which News Corp has a 78.8 per cent stake), Canal Plus lodged a lawsuit against the company in the California District Court seeking triple damages from losses of \$US1 billion - all from that Secarom.zip file on Al Menard's website.

NDS chief executive Abe Peled strenuously denies the Canal Plus claims. "This is not the suit of a cheated business seeking protection from piracy," NDS has told the court. "It is an attempt by an inept competitor to shift the blame for its incompetence, to damage its skilled competitor behind the shield of litigation privilege and to extract an unfair price in merger negotiations."

In many ways NDS is an accident of history. It grew out of a crash program in Israel to provide an encryption program for News Corp's Sky satellite service in Britain. In November 1988, five months after Rupert Murdoch had announced he was launching a British satellite service called Sky, rival BSB Holdings ran a full-page ad in the US magazine Variety urging studios not to sell movie rights to Sky: "Dear Hollywood, don't let Rupert feed your product to the pirates."

Australian consultant Bruce Hundertmark convinced Murdoch to use an unproved Israeli encryption company, News Datacom (later renamed NDS), which Hundertmark had badgered Murdoch to set up nine months before, to encrypt the Sky signal. The technology worked, but by 1991 the company was headed in Israel by an American-Israeli entrepreneur, Michael Clinger, who was a fugitive, on the run from an arrest warrant in New York. News Corp eventually forced Clinger out.

In the mid-1990s, NDS ran into two problems. The first was that pirates had cracked its smart card code. The NDS Videoguard system was based on an encryption algorithm developed by Professor Adi Shamir, one of the fathers of modern-day cryptology. But according to a former employee, for cost reasons the early cards did not carry the entire algorithm. This oversight allowed British video pirates to break the code. By 1994 there was a thriving piracy trade in counterfeit BSkyB smart cards. Soon after, in early 1995, NDS executives discovered they had a second problem: Clinger, the man they thought they had got rid of in 1992, had pulled off an international fraud that had cost NDS \$US19 million.

News Corp launched a massive world-wide investigation into Clinger's affairs, co-ordinated by British detective agency Argen Ltd and supervised by News Corp legal counsel Arthur Siskind. In 1996 News sued Clinger. The exchanges with Clinger became acrimonious. The court heard claims of death threats. Then in October 1996 Israeli tax officers raided the NDS offices in Israel, acting on claims by Clinger that NDS was evading tax. Five months later, Israeli police interrogated NDS chief executive Abe Peled for 16 hours over tapes of bugged telephone conversations the tax officers had found in his office.

Police also interrogated Reuven Hazak, the former deputy head of Shin Bet, the Israeli internal security service, who ran a private detective agency called Shaffron, which was working for NDS in the Clinger investigation. No charges were laid and both men claimed Clinger had planted the tapes. NDS later paid a \$US3 million no-blame settlement to the tax men. Hazak subsequently became security chief for NDS in Israel.

It was in 1996, when the investigation into Clinger was at its height and News Corp had learned the advantages of covert intelligence, that NDS quietly set up its own covert operation aimed at the pay-TV pirates. Besides Hazak in Israel, NDS hired Chris Morris as US director of special projects. Morris was a former army counter-intelligence officer who had run sting operations in North America for General Instruments to jail cable-TV pirates. In the UK, NDS later hired former Scotland Yard commander Ray Adams as director of security for NDS in Britain, after he was cleared by two inquiries into his links with criminal figures whom he had used as informants.

There was a second, secret arm to the NDS strategy. It was to put a group of hackers on the NDS payroll. It was known as the Swiss Cheese Group. Apparently NDS believed in this way it could keep abreast of developments in the hacking world. It also tapped the hackers' expertise to test its own products, and those of its rivals.

Germany was the most fruitful recruiting ground, among hackers associated with the Kaos Computer Club. NDS tried for two years to recruit its most famous member, Boris Floricic, a brilliant German hacker known as Tron. In October 1998, Floricic's body was found hanging from a tree in a Berlin park, with both feet on the ground. "We're always looking for excellent engineers, and we contacted him with a view to employing him as a consultant," NDS spokesperson Margot Field told The Guardian newspaper in December 1998. Among Floricic's papers, his father found an NDS invoice dated July 12, 1998, which read: "Hello Boris, here are the analog devices, good luck." Police say many companies tried to recruit Floricic. They concluded he committed suicide. Floricic had published a paper about hacking, or reverse-engineering, smart cards with Marcus Kuhn, a student at the University of Erlangen in Germany (now at Cambridge), who ran a user group called TV-Crypt.

In 1999 Kuhn co-wrote with another young hacker, Oliver Kommerling, what became one of the standard texts on how to reverse-engineer a state-of-the-art smart card, titled Design Principles for Tamper Resistant Smartcards, using acid treatments, microscopic probes, laser cutting, ion beam manipulation and other techniques. Kommerling says he has worked as a consultant for NDS since mid-1996, helping set up the NDS Matam Centre research facility in Haifa by early 1997, and recruiting and training all the Matam engineers. Another NDS recruit in April 1996 was a young hacker living in Germany, Christopher Tarnovsky. Journalists has located two 1995 postings to a UK Internet bulletin board which are signed Christopher Tarnovsky. They have an e-mail address from a US army base in Germany and ask for help hacking a D2Mac encryption chip: "I own a copy of the Black Book and have disassembled the code for dual & single chip but still am a little confused ..." Several hours later, he repeated the appeal: "Can anybody out there explain the EuroCrypt M/S packet structure a little bit to me!?! I have the source to single/dual chip version but the packets structure etc. is still UNKNOWN! ... I have the Black Book. That's not enough though."

Another hacker who knew Tarnovsky through Kuhn's TV-Crypt user group and ended up doing consulting work was Jan Saggiori, in Geneva. In 1996 Saggiori introduced Tarnovsky to a Canadian - Menard - who ran a piracy website called DR7, and later to another Swiss-based hacker, Vesselin Ivanon Nedeltchev, known as Vesco.

Saggiori says in his (Canal Plus) affidavit that he believed Vesco was working directly for Reuven Hazak at NDS in Israel last year. NDS found its biggest problem was in North America, where it provided smart cards for DirecTV, the satellite broadcaster owned by General Motors. NDS went hard after pay-TV pirates based in Canada.

Simultaneous raids by the Royal Canadian Mounted Police, US Customs and the FBI in November 1996 saw 60 people arrested for video piracy, but convictions were hard to come by. Canadian courts found it was not illegal for Canadians to pirate the US DirecTV signal, which by law could not be sold in Canada. By 1998, DirecTV's problems with piracy were so severe that it issued a formal notification to NDS that it was reconsidering its encryption system and examining its rival, NagraStar, owned by the Swiss Kudelski group, used by Echostar.

Almost immediately Nagra was also hit by a wave of piracy; *a coincidence?* The hacking community is full of finger pointing, and Nagra was told by some dealers that NDS had released Nagra's source code, which was published on DR7.com. Tarnovsky, who now lived in California, and his friend Menard fell under suspicion. Last May Echostar security officers used an associate of Menard's, Sean Quinn, to meet Menard in a hotel room in Vancouver, where they urged him to become a witness against NDS and Tarnovsky. But Menard vigorously denied that Tarnovsky had provided him with Nagra code. No further action was taken.

Friction also arose in Britain, with Internet speculation that NDS was linked to a piracy site, Thoi.com, also known as The House Of Ill Compute, which helped hackers make counterfeit smart cards for ITV Digital, a rival of BSkyB which uses the Canal Plus system. NDS has confirmed that UK security chief Adams paid several thousand pounds into the personal bank account of the man who ran the site. Adams claims he was not aware the Canal Plus software codes were on the site. Meanwhile, Canal Plus Technologies was also investigating how pirates had been able to flood the

market in Italy with counterfeit smart cards in late 1999. By mid-2001 Canal Plus's head of security, Gilles Kaehlin, believed he had tracked the leak down to a file posted on DR7 on March 26, 1999.

Earlier that month, Rupert Murdoch had met Jean-Marie Messier of Vivendi Universal, the controlling shareholder in Canal Plus. But talks to merge BSkyB with Canal Plus had broken down. News had been planning to invest in Italian pay-TV operation Stream SpA. Vivendi had been anxious that News stay out of Italy, to avoid competition with the Canal Plus pay-TV arm, Telepiu. In an affidavit filed in the Canal Plus court case, Kommerling, who now runs a security consultancy called ADSR, which is 40 per cent owned by NDS, said in early 1999 he was given a copy of a written summary of the Canal Plus code which had been extracted from a Canal Plus smart card by the NDS laboratory in Haifa. He later recognised the code file posted on the DR7 site as the same file. NDS employees told him the file had been supplied to DR7.

The file was posted on DR7 with a Readme text file which said in part, "This file has been downloaded from www.DR7.com ... We ask for nothing in return but a simple acknowledgement and thanks and those who redistribute as their own without reference to the source are true losers." In a second affidavit, Saggiori said when he downloaded the code from DR7 that weekend, part of the code was lost in the transfer. He asked Tarnovsky if he could obtain the missing file from Menard at DR7. Saggiori's affidavit includes a printout of an e-mail which he says Tarnovsky sent him with the missing binary file on March 28 as an attachment. It read: "Good news from up north here. Enjoy, keep for you please ... extremely top secret!"

By the middle of last year, Canal Plus says it had narrowed the source of its pirated smart cards to the DR7 file, but didn't know how it got there, when Kaehlin, the Canal Plus security chief, met Tarnovsky in London on August 15. On October 5 Kaehlin flew to California to meet Tarnovsky at his home in Carlsbad. In his affidavit filed in the Californian District Court, Kaehlin said Tarnovsky spoke of leaving NDS, but said it would be "extremely difficult for him to leave NDS because he was afraid of certain NDS employees". However, in what Kaehlin says was a "non-verbal method of communication", Tarnovsky said NDS was responsible for the publication of the Canal Plus code and that the code had been sent to him by Reuven Hazak via John Norris. Kaehlin says in his affidavit that he met Tarnovsky again in Santa Monica on December 16, when Tarnovsky told him, "he would tell the truth to the court if he were called to testify but that he would not be the whistleblower on NDS illegal activities, because he feared too much for his life and that of his family." In early January 2002, Tarnovsky sent Kaehlin a brief e-mail saying he did not want to talk to him any more. Norris in his (Canal Plus) affidavit says he has never had possession of a file titled Secarom.zip, and denies all of the Canal Plus claims. He says Tarnovsky also denied to him that he had supplied the file to DR7. NDS chief executive Abe Peled also denies the claims and links the lawsuit to an attempt to extort a higher price in talks to merge Canal Plus Technologies and NDS.

The colourful claims by Canal Plus are yet to be tested in court by cross-examination by the NDS lawyers. Even if Tarnovsky did supply code to DR7, which is yet to be proved, the Canal Plus case must prove that he was instructed to do so by NDS management. Otherwise he would be just another rogue employee.

Hackers out of the woodwork

If nothing else, this lawsuit is bringing hackers out of hiding. Hacker sites (such as www.dr7.com) have been filled with opinions (many heavily biased of course). The following is such an opinion and is included here as an example of the kind of rhetoric being posted on hacker and hacker-related web sites.

COMMENT:

Wow this is a very positive admission made by Mr. Oliver Kommerling for Canal + and while it has

been well known for quite some time that these codes and the Echostar information was released on DR7 from Mr. Chris Tarnovsky, formerly known as "Big Gun" or "BG" and "Von" " Shrimp" and other aliases by some of the ex-Admins on DR7, it was never admitted that it was NDS who actually did this. Mr. Tarnovsky, who is known to be a "bullshitter" and liar, had always claimed that this was done at NDS's request by Mr. Tarnovsky himself who claimed that HE is the one who hacked the codes. Many people on DR7 and especially Admins who may have been aware of this, did not believe Mr. Tarnovsky completely and we

believed that he had assistance in this. It was also claimed that he was under NDS protection in Canada and that NDS had the RCMP in its pocket and that anyone dealing in these cards for Echostar (Echo group) was not in any danger of being hassled by the RCMP. This seemed very true to many of us who knew that the RCMP had a very cosy arrangement with the NDS and thus DirecTV®, that the RCMP were flown to NDS headquarters (and DirecTV®) at NDS expense and had acted for the RCMP as a witness in many cases in Canada. They (the Government) called both Mr. Geoffery Kilfoyle and Mr. Art Sutherland (of Florida) in my case, for instance. Kilfoyle is an ex-Industry Canada employee and Sutherland is ex-Secret Service as they specialise in Ex-Government employees in their so called "security department". It certainly seems like the RCMP were again duped by NDS who are the subject of these civil (and possible criminal in effect) allegations, if they prove true. Judge Craig of the court in B.C. had said this (that the RCMP were DUPED) back in 1996 as well. It seems to me that a deal will be struck if this is true since the proof of this would totally destroy NDS as a business, leaving them only with the Murdoch companies as clients. They have already lost DirecTV® who will cease to deal with NDS once the current contract runs out. It is a fair assumption that this is not a coincidence. As Mr. Tarnovsky and Mr. Al Menart (DR7) will be deposed by Canal + in this affair and are sure to be called as witnesses at trial if NDS does not settle this, they will probably not lie since that may be a WORSE offence than having done the release. While Mr. Tarnovsky may be willing to lie for his employer NDS, its very doubtful that Mr. Menart will be willing to be charged criminally now that

other witnesses have spoken. If these witnesses confirm Mr. Kommerling's statement then any witness who lies may well be charged criminally by Canal + who do not seem to be fooling around, or by the court itself in California. When one takes a look at the people they wish to depose, including Mr. John Norris and Mr. Abe Peled, the NDS CEO, it looks like there will be a problem for several current and past NDS employees if they do not testify truthfully against their employer, given what they must surely know about this affair. These same people will undoubtedly be called to testify as well as several other Canadians who sold the Echo 3M code for DR7 (who had the writer) since he is very likely to have told them as well as others he told about this connection. At the testimony stage, where cross examination of witnesses comes in, it will be very difficult to keep the truth from being revealed. Especially if the courts have seized documentary evidence as was requested.

When it

comes to computers and documentation, there is almost always some revealing document to be uncovered that may have been forgotten. It looks to me like the truth will come out here even if NDS continue to try to deny it. If Mr. Tarnovsky actually did this, which he has stated in the past, it was at the request of his employer NDS who appear to be protecting him so far, and its much more likely that as Mr. Kommerling states and it was done in NDS lab in Israel where MANY of the witnesses to be deposed work. Mr. Tarnovsky was previously known for making "battery card" files for DirecTV® hacks in the P1 era and we doubt his abilities to do these much more sophisticated jobs on the Canal + and Nagra cards used by Echostar. The use of the Echo 3M card and that it was DR7 who wrote these cards sold by Hitec, Koinvision, Discount Satellite and the new frontier group is very well known. As at least one of the owners of these groups are in the USA its very likely that the people who ran these

groups will be brought into the lawsuit. It is widely known who SQ, AS, DD and SF are to a very wide array of people. You can be very sure that Canal +, who did a very thorough investigation, know exactly who and where these people can be found. Even some of their unfortunate banking connections in Antigua who appear to have gone bankrupt now, leaving inadequate records for the authorities.

...

Perhaps the current generation and design of (television and other) smart cards is "dead." And any new smart card versions released are at best "patches" designed to "buy more time" until the next

totally new level of encryption technology can be perfected for commercial use. With NDS booted out by DirecTV, and every sign suggesting NDS competitors (such as Canal Plus) are also having a tough time staying ahead of hackers, what is next? Is pay-TV encryption a dinosaur? Is NDS over valued even after dropping 60% of its market value since March 12?

Three reports that suggest this may be the next technology plateau.

A collection of consumer electronics manufacturers, Hollywood studios, high-tech companies and satellite operators formed a group that will develop a new technology standard for protecting high-definition video and digital audio. The businesses said the standard, called high-definition multimedia interface, or HDMI, will be designed to thwart pirating of super-high-quality images and sound as they are transmitted within a living room from satellite and cable-tuner boxes and digital videodisc players to high-definition television sets. Entertainment companies consider copy protection for the digital interfaces between consumer electronics gadgets to be an essential step before high-definition content becomes widely available. Matsushita Electric Industrial Co.'s Panasonic, Sony Corp., Hitachi Ltd., and Toshiba Corp. are among the consumer electronics firms supporting the working group that will develop HDMI. Two movie studios, News Corp's Fox and Vivendi Universal SA, and two satellite operators, Hughes Electronics Corp.'s DirecTV and EchoStar Communications Corp., endorsed the effort, as did high-tech concerns Intel Corp. and Silicon Image Inc. Companies involved in the effort said HDMI is a more-advanced version of an earlier high-definition protection standard known as digital video interface, which was primarily designed for the playback of high-definition programming on personal computers. HDMI, in contrast, is geared more toward consumer electronics devices. The new standard will combine video and audio connectors between devices into one wire, eliminating the nest of connectors required between audio-video components today, said Steve Tirado, chief operating office of Silicon Image.

NDS Group down 23% After Report Of Plans For Rival Tech. American depositary receipts of NDS Corp. (NNDS) sank 27% following reports that a group of Hollywood studios and consumer electronics, satellite and high-tech companies are working to create a new technology to prevent the piracy of high-definition TV programming, the same technology that NDS offers. The Wall Street Journal reported that the businesses have formed a consortium to develop a standard called high-definition multimedia interface, or HDMI, that will prevent non-subscribers from stealing digital cable or satellite images. HDMI, according to the report, is described by the consortium as more advanced than an earlier high-definition protection standard known as digital video interface, which was primarily designed for the playback of high-definition programming on personal computers. Instead, HDMI is for use on consumer electronics devices. The news may arouse concern that a rival technology could threaten NDS' ability to keep its customers, such as Cablevision Corp. (CVC), with which NDS signed a contract in January. Earlier in April, Hughes Electronics Corp.'s (GMH) DirecTV ended its agreement with NDS, saying it would no longer use NDS encryption platform, and would move toward providing in-house conditional access services. DirecTV, according to The Wall Street Journal article, is one of the companies supporting the work group that will develop HDMI. NDS is also embroiled in a dispute with Vivendi Universal SA's (V) Canal Plus, whose accusations have hurt NDS' ADR price significantly in the past weeks. Last month, Canal Plus sued NDS, alleging it directly aided in the widespread pilfering of digital TV broadcasts. ITV Digital, owned by broadcasters Granada PLC (U.GAA) and Carlton Communications PLC (CCTVY), has also complained that NDS distributed information used to create pirate decoding cards. Company officials weren't available for comment.

How "smart" is your ID card? Allies of "smart cards"--credit card or ID cards with small computer processors--are improving the technology in hopes of hastening its broader use. Smart cards offer advantages such as better security to identify their carriers and incentives to keep customers coming back to the same store, but getting consumers and companies to switch to the new technology has been an uphill struggle. At the CardTech/SecurTech conference in New Orleans, advocates announced a host of improvements. SchlumbergerSema, a Schlumberger business unit that makes and sells smart cards, introduced ICitizen, a new smart card with features such as security and counterfeiting resistance. It also has large storage capacity for recording data such as fingerprints or other biometric data, driver's license numbers, health data and digital signatures, the company said. The encrypted data can be protected with simple personal identification numbers or more complicated

biometric data. The SchlumbergerSema card can also run programs written in Java Card, Sun Microsystems' version Java software for smart cards.

Sun, meanwhile, introduced version 2.2 of the Java Card technology. Java Card lets programs written to its specifications run on many different smart cards, regardless of what processor the card uses. Java allows smart cards to run programs for encryption, authentication of fingerprints, and other tasks. The new version of Java Card allows better control over how the cards use memory. It also offers improvements for tapping into wireless communication standards such as the Wireless Application Protocol and for better debugging tools to make writing programs easier, Sun said. Visa, another company at the conference, said it will offer centralised services to help card issuers and their merchant business partners try to keep customers returning. Four banks--First USA, FleetBoston, Provident and Retailers National Bank--have issued more than 10 million Visa smart cards so far, Visa said. MasterCard, meanwhile, announced its published specifications for the MasterCard Open Data Storage interface, which allows its banking partners to offer customers better management of personal information stored on the card. That information can include shipping addresses, phone numbers, username-password combinations, and receipts, MasterCard said MasterCard's smart card strategy supports the Java Card software as well as the Multos smart card operating system.

Uncrackable encryption: It's no longer just sci-fi. When I first heard about the encryption technique developed by Dr. Richard Hughes, it sounded like science fiction. After he explained it to me in detail, it still sounded like fiction. Imagine, if you will, a means of delivering encryption keys that is so secure that it's impossible to access because doing so would violate the laws of physics. In other words, the delivery method is so secure, it's protected by the very fabric of the universe. If that doesn't get your attention, think about this: What Dr. Hughes is working with is a way to encode information on individual photons. He then sends these encoded photons to a receiver that measure their characteristics and determine from those characteristics the data they represent. That's right: He's imprinting information on individual subatomic particles. What makes this so secure is that the information can be encoded in several ways. If someone were intercept these photons, only one of the possible encoding methods could be seen. If that method contain the needed information, the eavesdropper couldn't then look at the information that was encoded differently. So why couldn't a hacker occasionally determine the encoding method by trial and error? To do so would be pointless, because hackers could never be sure they were seeing the real data, and it would violate the Heisenberg Uncertainty Principle of quantum mechanics if the hacker tried to look at both types of polarisation on the same particle. Add to these complications that the mere act of observing the photons in their path changes them, and that the change is immediately detectable by the recipient. Here's how all of this works. Dr. Hughes, who works in the physics division of the Los Alamos National Laboratory, creates photons using a very attenuated laser. He's able to choose the polarity of each photon so that, for example, a vertical polarisation represents a 0 and horizontal polarisation a 1. Or, you can use opposite diagonal polarisations. The order of the polarization is varied randomly, but the sender has already sent the sequence to the receiver. That way, the receiver doesn't have to look at a bunch of other photons in search of information; it just looks for the information coming from the transmitter. The beauty of the method is that even if some hackers knew the order as well, they couldn't gather information without being detected. Why? Again, Heisenberg: You cannot observe a subatomic particle without changing it. When particles that have been observed arrive at the receiver, their bit error rate is very high, alerting the receiver that the data stream is being observed. As a result, the sequence can be changed immediately, regaining the security of the transmission. Nice theory, right? But using polarised photons for encryption is more than just a theory. In fact it's already working in at least two test installations: one is run by BBN Networks and Harvard University the other by the Army and Navy Research Laboratories near Washington, D.C. Both transmit the photons over optical fiber. But transmitting photons over optical fiber is limited to about one km, because using repeaters to strengthen the signal would introduce anomalies similar to those of eavesdropper. Dr. Hughes thinks the delivery method needs to go beyond that. "A much more compelling application is by transmitting through the atmosphere," Dr. Hughes explains adding that he's been able to do single-photon communications through the air in daylight with an acceptable bit error rate. No need to lay all that fiber-optic cable anymore. "The trick," he says, "is to find the single photon against the background." It sounds like a feat requiring equipment only NASA could afford--in fact, transmitting encryption

keys to satellites is being tested--but Dr. Hughes says he's mastered "free-space quantum cryptography" using commercial off-the-shelf components. Even better, you can buy this now. A Swiss company named id Quantique is already selling a device performs over fiber networks what it calls quantum key distribution. While the wireless optical version Dr Hughes is testing isn't available now, he says that at least two companies are working on commercial versions. Once these products are available, you can be confident that your communications are secure. Unless someone starts messing around with the universe, anyway.

Seen in a local NZ News group. Yesterday was the second visit I have had from a Sky TV salesman hoping to sell me a pay TV subscription. I told him that he was the second salesman to have visited in just a few weeks, and that I had not changed my mind; I still do not think that anything on television is worth paying for. He then told me that "people will keep on calling" until I had taken out a subscription.

Today I phoned Sky TV and asked to be put through to their door to door promotions manager. The man I spoke to confirmed that it is indeed true, the spammers will keep calling until a subscription is confirmed. I asked him how they knew I was not Sky subscriber. He explained to me that they have 2 databases. One was their own list of paid up subscribers, and the other was supplied to them by the Department of Statistics which lists every street address in the country. The door to door spammers (which they tell me are individual contractors) are supplied with lists of addresses taken from the Dept. of Statistics' records minus their own.

I also asked whether it would be possible for my address to be removed from the spammers' lists. He said: "I'll see what I can do, but I'm not promising anything". Translating that from salesman-speak to plain English turned up a definitive "no".

What I would really like to know is whether Sky TV are the only company to embrace this intrusive policy of sale by attrition, or has this method become fashionable with other companies as well? If this sales technique catches on, I expect that many people will notice a substantial increase in the number of uninvited visitors, many of whom will be trying to peddle a product or service that has been previously declined on more than one occasion. Maybe I'll just invest in a "No Hawker's" sign. Can any door to door salesman sell me one of those?

Meanwhile, the world's first terrestrial digital pay-TV broadcaster, iTV, is done. Kapoot. Gone. A victim of card hacking piracy and its own internal decision making process, digital terrestrial television has now suffered a major setback in the UK. First the lead up, and then the bad news.

ITV Digital is preparing a £100m lawsuit against a spin-off of Rupert Murdoch's News Corporation after accusing it of helping fund hackers who published on the Internet secrets about its pay-TV technology. The struggling digital television firm says more than 100,000 forged smart cards ended up in circulation giving free access to its programmes and depriving it of millions of pounds of revenue. In a move that underlines the increasing bitterness between ITV Digital and Mr Murdoch, the mogul yesterday branded as immoral attempts by the owners of the business, Carlton and Granada, to renegotiate the terms of its £315m broadcasting deal with the Football League.

Representatives of the league's 24 first division clubs are due to meet in London to discuss legal action of their own against ITV Digital, which says it can no longer afford the deal. Keith Harris, the league's chief executive, has pledged to sue ITV Digital's owners Carlton and Granada for £500m if they fail to pay the contract in full. Some clubs are understood to be ready to push for a settlement in an attempt to avoid a protracted legal battle that would leave many of them facing bankruptcy if it failed.

Mr Murdoch said: "What Carlton and Granada are trying to do is just immoral. It is not as though the owners don't have the money; these are two very big companies."

Following a two-year investigation into NDS, ITV Digital says it has clear evidence that the UK technology company, 79% owned by News Corporation, helped fund hacker websites that spread its secret pay-TV codes to pirates. Lawyers for ITV Digital want to join a \$1bn legal action against NDS in the US, launched last month by its smart card supplier, Canal Plus. The decision on whether to join the suit, and on what basis, will be taken by Nick Dorgan, the Deloitte & Touche administrator who was appointed (last week) to try to save the platform. NDS has dismissed the allegations against it as "outrageous and baseless", and is preparing to counter-sue. It did admit to the Guardian that its head of security, former Scotland Yard commander Ray Adams, helped fund a website called The House of Ill

Compute, which published ITV Digital codes. Mr Adams is the representative of NDS and ITV Digital's arch-rival, BSkyB, on Aepoc, a European body set up to tackle pay-TV piracy. The case is expected to be heard in a Californian court.

In the meantime Mr Dorgan will continue to attempt to renegotiate the contract with the Football League and ITV Digital's other suppliers. If he cannot succeed, Carlton and Granada are likely to put the business into liquidation. Although the league's 72 clubs publicly insist they will not renegotiate a contract that ITV Digital says it now cannot afford to pay, a rift is emerging between clubs ready to settle and those that want to fight on. The chairmen are expected to demand to see the legal opinion on which its case would be based and the short-form version of the broadcasting contract. The full version of the agreement was never signed and lawyers say this could invalidate the league's claim.

Several potential buyers are circling ITV Digital in case Carlton and Granada pull the plug.

(As many as 60 prospective buyers for all or part of ITV Digital have come forward. Administrators Deloitte & Touche announced they were ready to break the company up and sell off its assets, as money to keep it going was running out. Culture Secretary Tessa Jowell says the company's collapse does not spell the end for the Government's hopes of switching the whole country to digital TV by 2010. The technology's future in Britain is still "positive", she says. But she made clear that there would be no financial bailout for ITV Digital or the Football League, which is owed £178.5 million in broadcasting fees. While the Government would do "all we can" to support clubs facing insolvency and players who lose their jobs, it would not intervene in "what is essentially a private matter between a company and its creditors", she said.)

Coop's comment: This UK web site posting attempted to advise the 1.2 million users of iTV Digital what their options might be with the closure of the service eminent.

WHAT ITV DIGITAL'S SITUATION MEANS TO YOU

If you are an ITV Digital subscriber, by the time you read this, the most likely outcome of the crisis is that your screen will be blank on Sky 1, E4 and so on. You will continue to receive all of the free-to-air channels such as BBC1, ITV1, BBC Choice and more. But while this is the most likely situation, it's far from certain.

The reason is that while ITV Digital is to be broken up, its channels belong to the companies that make them: E4 comes from Channel 4, Sky 1 from BSkyB, for instance. ITV Digital is meeting with these programme providers today (Friday 26 April) and it is possible they will each take what is being called 'a payment holiday': that they will continue to supply the channels without payment until the situation is resolved. At some point, though, they are likely to cease transmission and the moment that these pay channels are gone, the ITC will revoke ITV Digital's licence to broadcast. On Monday 29 April, administrators will put the company's assets (the set-top boxes, the viewer subscriptions) up for sale. The sale is expected to take six weeks and if it fails to attract buyers, ITV Digital will be liquidated. During that period, though, it is possible that an interim broadcaster will take over operations and keep more than the free-to-air channels running.

Note that Sky Digital and cable viewers are unaffected by this: even ITV2 will continue, though ITV Sport is in some doubt.

Meanwhile, Canada is up in arms. By a strange set of circumstances, Canada's laws have allowed individuals and companies to create piracy smart cards and sell them to Canadian users without consequence of the law. The Canadian law has repeatedly been tested in court and in 2000-2001 alone 21 judges ruled that grey market products (unauthorised smart cards) which allow Canadians to view the USA's DirecTV (or Echostar/DISH) services were not illegal. The judges uniformly found the (Canadian) law against grey market cards applied only to pay-TV services "authorised for distribution within Canada" and DirecTV as well as DISH were not authorised in Canada. A number of very vocal spokesmen (and spokes women) have risen throughout Canada above the din - which is considerable with estimates running as high as 700,000 Canadian homes watching DirecTV or Dish (or both). The Supreme Court of Canada was scheduled April 26 to release their decision after an appeal of a lower court ruling from a judge who found no law was being violated. Here is the work up to that decision, which follows.

Signal theft coalition formed; as many as 660,000 stealing TV signal. A full court press from the cable, satellite and broadcast industry is about to greet the federal government, where a new coalition

is insisting the politicians to do something about satellite signal theft. A total of 15 companies and organisations have banded together to form the Canadian broadcast industry coalition. The Canadian Cable Television Association is leading it and recently completed a survey of 1,000 people in the 519 and 905 area codes in Ontario to ask them about their television providers. Of the 204 satellite users in the surveyed group, 66% said they get Star Choice or ExpressVu. A total of 28% either refused to answer (6%), could/would specify no company (16%) or said they had DirecTV (6%).

Another question put to the whole sample found that many reported access to supposedly unavailable channels such as USA Network (12%), Turner Classic Movies (13%), HBO (21%) and ESPN (29%). Then again, though, 25% of cable customers and 49% of legal DTH customers reported they had access to ESPN, so perhaps TSN's recent rebranding in the image of its corporate partner has worked well. However, a large proportion of both legal cable and satellite customers reported access to the other three unavailable channels mentioned above.

The coalition used the survey data to extrapolate that nationally, between 520,000 and 660,000 people are using illegal dishes, or in the coalition parlance, have "unauthorised satellite systems active in Canada." The issue is of vital importance to the viability cable operators and broadcasters in Canada. Cogeco Inc. president and CEO Louis Audet told financial analysts during his company's fourth quarter conference call. Calling recent customer losses to satellite "the worst in our history," Audet called on the Federal government to change things. "We are meeting today with a variety of governmental departments, impressing on them that the black market is leading to the loss of Canadian viewers and that would apply to broadcasting as well as cable," he said. While the crux of the problem is DirecTV hackers, a growing number are stealing ExpressVu signals and Audet said it was incumbent on all satellite providers to step up security, saying they "have a responsibility to improve their encoding."

The Supreme Court of Canada is scheduled to announce its decision on the Bell ExpressVu vs. Rex case.

At issue is whether Canada's estimated 700,000 to one million grey or black-market satellite viewers are breaking the law or enjoying a freedom of choice and information guaranteed under the Charter of Rights and Freedoms. The decision will have a major impact on Canada's two sanctioned satellite providers, Bell ExpressVu and Star Choice. Will the federal court reverse the stand taken by Supreme Courts in B.C. and Ontario and outlaw signals coming from south of the border? Those courts ruled that there is no legal basis to prevent Canadians from receiving U.S. satellite programming. In other words, why order The Osbournes on MTV Canada when you can catch it months earlier on the real MTV?

Bell and Star Choice have waved the flag, demanding that sanction and sovereignty be asserted. But is this cultural nationalism or business opportunism? And what about all those Americans (or snowbirds living in Florida) who might want to subscribe to Bell or Star Choice stateside? Isn't that what free trade was all about?

The ramifications are endless. If the court sides with Bell, the RCMP could be back in the dish-hunting game. If the ruling favours grey dish sellers and owners, the feds will harass you no more. Maybe. Both sides are ready to fight on, depending on which way the decision goes. Bell has vowed to lobby Ottawa to rewrite the flawed Radio Communications Act to tighten loopholes and protect Canadian business interests. And you can bet that DirecTV, the major U.S. satellite provider (owned by General Motors), has lawyers on the decision.

Keeping an eye on them all is Ian Angus, a Toronto-area communications lawyer who has a banner ad on the grey dish-friendly Legal Rights Satellite Organisation Web site (www.legal-rights.org). Their slogan: "Satellite rights in Canada is a David and Goliath battle that is being won by David." Over the past six years, Angus has represented many clients who have battled over grey and black-market satellite rights. He sees tomorrow's ruling as "half the big decision" in terms of the satellite picture. "Trying to slam the door shut on U.S. satellite signals is an Iron Curtain idea tantamount to building a 10,000-mile-high wall at the border," says Angus. "In today's wired world, it just can't work. You can't put the genie back in the bottle."

And the reports (3 of many-many) regarding the Canadian court decision.

Court rules on 'grey-market' satellite decoders. Unlicensed providers selling decoders for foreign-based satellite signals are breaking a federal broadcasting law, says Canada's top court. The

Supreme Court of Canada ruled 7-0 (April 26) that such businesses do violate the Radio communication Act that outlaws the unauthorised decoding of an encrypted signal. The judgement is a victory for Canadian satellite giant Bell ExpressVu which is suing a small British Columbia satellite provider. However, the high court left it up to the so-called grey-market satellite providers to make a strong case in court that the federal law violates freedom of communication guaranteed under the Charter of Rights and Freedoms.

Hundreds of thousands of grey-market satellite users across the country were awaiting the outcome of the case that pitted a small British Columbia business against industry heavyweights. ExpressVu appealed to the high court after failing to persuade lower courts to grant an injunction against Can-Am Satellites, based in Maple Ridge, B.C. Can-Am and other grey-market businesses feed subscribers signals directly from the United States and other countries. In turn, customers pay in American dollars and are issued a U.S. address. ExpressVu lawyers argued that Can-Am is luring business away by enticing consumers who might otherwise obtain a similar service from ExpressVu. That's unlawful, they said, because ExpressVu and StarChoice, owned by Shaw Communications, are Canada's only licensed direct-to-home (DTH) providers.

Lower courts weren't convinced. The B.C. Court of Appeal ruled in September 2000 that the Radiocommunication Act does not bar Can-Am from offering Canadians access to foreign signals. A separate Ontario Court of Appeal judgement last April quashed an RCMP search-and-seizure warrant obtained for satellite dealer Tech Electronics. The court concluded there were no criminal offences occurring at the business that sold grey-market systems. Lower courts have said broadcasting legislation applies only to signals that originate in Canada. They also cast doubt on whether the punitive aspects of the Radiocommunication Act were meant to catch people intercepting foreign satellite signals. Can-Am lawyers argued Canadian law cannot reasonably ban the decoding of broadcasts from other countries. Such a prohibition would violate rights to free expression and communication guaranteed under the Charter of Rights and Freedoms, they said.

While grey-market proponents hail freedom of choice in a free market, the two authorised satellite distributors, cable, broadcast and film representatives cite cultural consequences. They say unlicensed grey-market distributors don't support the Canadian broadcast system, which requires payment from licensed companies to maintain Canadian content. The broadcast giants warned earlier this month that unlicensed satellite providers are draining millions of dollars from licensed Canadian companies. Industry critics say that self-interested broadcasters want to maintain control over the viewing market so they can make more money.

The numbers of Canadian viewers bypassing licensed satellite providers has been estimated at anywhere from 200,000 to more than one million. Broadcasters have said the grey market is sucking about \$400 million a year out of the Canadian system.

Hands up — and drop that remote control! After half a decade or so of lobbying and legal manoeuvring, the satellite broadcasters now finally have a Supreme Court of Canada ruling they can use as a stick to beat up "grey market" satellite dealers — and even individual users if they wish. Even now, cruisers full of RCMP officers may be roaming through your neighbourhood looking for evidence of illicit dishes. Heritage Minister Sheila Copps, it seems, has won her battle to protect Canadians from receiving unclean American satellite signals. On April 26, the Supreme Court struck down a British Columbia court decision that said Canadians receiving U.S. satellite signals were not committing an offence under the federal Radiocommunication Act. The B.C. court said the same thing several other lower courts in various jurisdictions have said in similar cases, which was that the act was designed to prevent Canadians from receiving Canadian broadcast signals from an unlicensed provider, not from paying for and getting U.S. signals. The Supreme Court disagreed, however. In effect, it said the exact opposite of what the B.C. Superior Court said in its ruling. In the 1999 decision, the B.C. judge said that section 9.1(c) of the act did not cover Canadians getting U.S. broadcasting, because if it was meant to do so then legislators would have spelled that out in so many words. The Supreme Court, meanwhile, said that because the act doesn't specify whether it refers to Canadian or U.S. signals, then by definition it covers both. Whether the Supreme Court's interpretation is the correct one or not is mostly irrelevant — it is the highest court, and so by definition its ruling is now the law. Whether it is a good or appropriate law, however, is a completely different question. Should there be a Canadian law that erects a giant wall at the Canada-U.S. border, so that Bell

ExpressVu and Star Choice can have the satellite market to themselves? Should Canadians be prevented from paying for and receiving lawful U.S. signals?

For many — including, obviously, the hundreds of thousands of Canadians who have signed up for DirecTV or the DISH network — the answer is no. Television and radio broadcasts, after all, don't respect national borders and never have, and it's not clear why they should be forced to simply because ExpressVu and Star Choice say they should. Canadian residents who live near the border (which describes a large part of the population) are used to tuning in to U.S. radio and TV stations as a matter of course. What difference does it make whether they use a dish or a piece of wire?

ExpressVu and Star Choice like to blur the line between the grey market and the actual black market, to the point where they cite a single figure of 700,000 as the number of users of both grey and black market dishes, and hazard a guess as to which is which. But there is a fairly clear distinction: grey market users pay all the required fees to the U.S. distributor for the dish and the service, just as U.S. residents do, while black market users buy a dish and then use "cracked" access cards.

The two Canadian companies argue that they pay for the rights to various programs from U.S. distributors, and that bypassing them and getting the programs from a U.S. source should be illegal. Why? Because they say so, that's why. Apart from the fact that grey market access makes the high prices charged for satellite access seem less attractive, it's hard to see what sort of actual crime is being committed. Why not ban Canadians from buying U.S. magazines, or buying books from a U.S. Web site like Amazon? Satellite fans point out that the policy of cracking down on the grey market tends to avoid a couple of things: one is the tens of thousands of Canadians who are still using those old-fashioned "C-band" satellite dishes, the ones that are six feet across and can be moved to target different satellites. Why aren't they mentioned? Because there aren't that many of them, for one thing. Star Choice and ExpressVu are more concerned with the hundreds of thousands of urban residents who use illicit dishes. Another thing that doesn't get mentioned much is what might be called the reverse grey market: those Canadian and U.S. residents who sign up for Star Choice or ExpressVu either through a fake Canadian address (set up through a broker such as Freewaysupport.com) or who get a second dish and receiver in Canada to take down to their winter place in Florida. There aren't many of those either — not to mention the fact that there is no U.S. law that blocks foreign signals the way we do.

But those are moot points. The central issue is whether a law-abiding Canadian citizen who pays for a satellite dish and receives signals that originate in the U.S. is committing a crime or not. According to the Supreme Court and the government, the answer is yes. According to most other rational yardsticks, however, the answer is probably no.

The cops are here, they want the dish. Come and get it! My U.S. satellite dish, for which I pay a pretty penny a month to subscribe, is up and running. I had it installed a few years ago. One reason was to pick up (and pay for) some programming otherwise not available in Canada. But mainly it was a pathetic act of small-time defiance against the big-time political-corporate collaborators who are perpetually attempting to restrict the freedom of Canadians to watch, read and listen to whatever they want. The romantic image of the RCMP possibly arriving at the front door one night to rip out the dish and lay charges was too appealing to ignore. It's not often in life, after all, that one gets the opportunity to give the finger to such a stellar collection of hypocritical, self-serving and manipulative nationalists. Look at this list of collaborators whose sole intent is to capture consumer dollars and cheap nationalist votes: The Canadian Association of Broadcasters and its members; the Canadian Cable Television Association and its members; Rogers and Shaw; Bell ExpressVu and its parent; a string of industry ministers that include John Manley and Alan Rock; the Canadian Radio-television and Telecommunications Commission; the Canadian Film and Television Production Association; scores of bureaucrats, patronage seekers and attorneys working for the federal government and industry associations; the RCMP; and, the strongest motivating presence of all, Sheila Copps. All of these protectionists and legal charlatans kept in high agitation for only a couple of dollars a day; now that's satisfaction.

The RCMP, disappointingly, has yet to show up. And now that the Supreme Court of Canada has ruled in favour of the political-corporate collaborators, the odds are still slim that federal police will soon break down the door and confiscate the equipment. In a somewhat artificial argument that turns on the parsing of half a dozen words in the 1992 Radio communications Act, the court concluded that

the Act prohibits the decoding of "all" encrypted program signals except those signals "received" from authorised and licensed transmitters, i.e., Bell ExpressVu and Star Choice.

Ottawa, Bell ExpressVu and the RCMP have jumped to the conclusion that the court ruling gives them permission to raid, charge, prosecute and harass out of business the companies that sell the equipment that does the decoding. Really? I'm no lawyer, but a reasonable reading of the decision suggests the RCMP has no such authority. "I can only conclude," wrote Mr. Justice John Iacobucci in the unanimous decision, "that Parliament intended to create an absolute bar on Canadian residents decoding encrypted programming signals." And in the final disposition, he writes that the act "creates a prohibition against all decoding of encrypted programming signals, followed by an exception where authorisation is received from the person holding the right in Canada to transmit and authorise decoding of the signal." In other words, it is illegal for Canadian residents to receive decoded signals. But there is no court prohibition against selling the equipment used in the decoding. It is as if the court had ruled on a law that prohibited the smoking of marijuana without outlawing possession or sale of marijuana. A man standing on a corner with a Glad bag full of marijuana would not, under such a law, be breaking the law if he were not himself smoking it.

Beyond this admittedly technical uncertainty -- never a deterrent to this crowd in the past -- is the matter of the Charter of Rights and Freedoms. "It may well be," writes Justice Iacobucci, "that when this matter returns to trial, the respondents will make application to have [this section of the Radio communications Act] declared unconstitutional for violating the Charter." The specific freedom mentioned by the court is freedom of expression, one of the fundamental freedoms under Charter section 2, clause b: "freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication."

Such a Charter test is likely to be filed within days, along with requests for court stays of enforcement to prevent the RCMP and the government from mounting a national jihad against distributors of satellite dishes. It will take another couple of years to move a Charter case through the courts to test the validity of broadcasting laws that are mired in anachronistic provisions and outdated technological models.

At one time it could be argued that Canada had limited public airwaves and there was a need to set up a protective regulatory regime. But the airwaves are no longer limited. The encrypted satellite signals, along with digital cable and other digital modes of transmission including Internet, create unlimited "broadcast" capacity. The entire Radio communications Act rests on technological quicksand and is unenforceable, no matter how many RCMP officers are dispatched to harass the population. The RCMP arriving at the doors of Canadians, and satellite distributors, to seize systems and jail people would be identical to the RCMP prosecuting distributors and readers of The New York Times, Vanity Fair and Rolling Stone. It's unimaginable. But it may happen. I'm ready.

...
End of big bucks for pay-TV sports? With every aspect of pay-TV's money losing formula under intense scrutiny, the large dollars being paid for professional (and some amateur) sporting events was only a matter of time. With the UK's ITV digital service closing down or being divided into its assets because it is facing a huge unfulfilled contract for British sport coverage, the financial handwriting is on the board. The bottom line - money being paid for sport coverage is about to go down, perhaps rapidly. Rocketing salaries to players, big bucks to field elaborate and state-of-the-art digital production vans, major dollars spent on promotional activities are all at risk. In Australia, News Corp is cutting its losses and divesting of an ownership interest in the Canberra Raiders. Next to go will be (News Corp) financial interests in the North Queensland Cowboys and Melbourne Storm. In Germany, News Corp's investment in sport is costing it millions in losses. In the United States, News is taking a US\$1.1 billion "write down" on NFL (National Football League) expenses. All of this bodes badly for future sport coverage on pay-TV, but in fact it has been the escalating prices paid by Murdoch controlled pay-TV broadcasters which has driven the sport industry for the last decade. In effect, they paid too much for what they bought creating a false level of funding for the sporting clubs and players. And now it appears the good years are old.

Satellite delivered Internet is NOT the answer. After five years of trying to be financially and technically successful, the folks who would deliver Internet and high speed data to millions of world homes have decided it is not a viable business plan. In New Zealand, IHUG appears to have reluctantly

come to the same decision while in Australia, the kind of subscriber uptake required for the Telstra offering has never materialised. Read what follows carefully and think twice before investing your money.

Thinking about getting broadband Internet access by satellite? Well, consider carefully, because the people who supply the service aren't sure it's financially sound. This was the message that pervaded Satellite 2002, the annual Satfest held this year in Washington, D.C., in March. In session after session, panellists bemoaned the problems facing satellite broadband, and wondered if a standalone service was such a good idea after all.

"When it comes to broadband over satellite, it is rocket science," explained Allen McCabe, assistant vice-president of U.S. field sales, at Hughes Network Systems' (HNS) consumer division. HNS owns DirecWay, the satellite system that downloads data at 400Kbps, and uploads from home users at 128Kbps. To date, DirecWay has about 100,000 users. It's not just the equipment that is complex, added Jim Grandahl, StarBand's vice-president of sales; there's also the finesse required to install it properly. (StarBand is a U.S.-only satellite broadband provider, with 40,000 subscribers.) After all, there's a big difference between factory-trained technicians installing a corporate satellite site, Grandahl noted, "and John in a pickup truck hooking up to God knows what kind of computer." To make matters worse, many satellite broadband companies are subsidising the cost of their consumer equipment, in an effort to compete with DSL and cable modems. Worse yet, the money they're spending on customer support often "costs more than the entire revenue stream you get from the customer," said John Hanes, senior vice-president of Pegasus Communications.

Grandahl echoed this, saying, "If customers are calling you for help once or twice a month it's difficult to make money."

It certainly is. In fact, StarBand is currently losing US\$70 per subscriber per month, said Steve Blum, president of Tellus Venture Associates. So why is satellite broadband in such a fix? Beyond the problems listed above, the concept itself is fundamentally flawed. The reason: satellites are relatively cheap to use for broadcasting simultaneously to millions of people. Known in the business as "point-to-multipoint," this approach works out to a minimal cost per user, which is why Bell ExpressVu and Star Choice are succeeding in the DBS (direct broadcast satellite) TV market.

However, the Internet access business is what's known as "point-to-point." In plain language, it's one channel serving one user, and that's it. Here, there are no economies of scale for satellite broadband carriers, as there are with DBS. As for ground-based networks? Well, they have an edge when it comes to point-to-point traffic. First, it's cheaper to install fiber optic cables than it is to launch a satellite. Second, upgrading is also cheaper and easier. Need more capacity? Just add another cable! In contrast, a satellite is made up of a limited number of "transponders"--combined receiver/transmitters that pick up and then beam signals back to earth--each with a limited 36 MHz of available bandwidth. As for increasing capacity by sending up another satellite, in round numbers, this will cost you about half-a-billion. Not cheap.

Then there's the business case: to make money, each transponder has to serve between 15,000 and 20,000 users, said Blum. This is tough enough with current consumer demand, he said. However, add in video streaming--with each channel demanding 200Kbps--and "it kills the model."

So what happens next? Well, the satellite industry believes satellite broadband will thrive where there's no alternative, like rural and remote areas. Meanwhile, for the rest of the market, the key will be to team up with terrestrial network providers, to offer a so-called "hybrid solution."

As for consumers? Well, it's not likely that DirecWay will leave you out in the cold anytime soon. However, DSL and cable modems are undeniably operating in an easier business climate. As a result, they have a better chance of being there in the years ahead.

The end is near.

Coop's Technology Digest will cease publication as a ten-time per-year creation effective with our August 2002 edition. This is issue 88, the final issue *should be* number 91. Renewal notices accompanying this issue have been dollar-adjusted to reflect ONLY the issues remaining. No new subscriptions are being accepted at this time. Our SatFACTS publication (May 2002 is #93) will continue ... until?

